2. Structure des corps (commutatifs) finis

Notation générique : soient $p \in \mathbb{P}$ et $n \in \mathbb{N} \setminus \{0\}$

$(K, 0, +, *, e)$, ou simplement K, désigne un corps fini de caractéristique $\mathrm{car}(K) = p$ et de cardinal $\mathrm{card}(K) = q = p^n$.
Hypothèse provisoire : K est commutatif.

1. K comme ensemble des racines de $X^q - X$
2. $(K^*, *, e)$ est un groupe cyclique
3. $K = \mathbb{F}_p(\alpha)$, *i.e.* K admet un élément primitif sur $\mathbb{F}_p$
4. $K = \mathbb{F}_p[X]/(P)$, où $P \in \mathbb{F}_p[X]$ est irréductible
5. Les sous-corps de K
6. Le groupe des automorphismes de K est $\mathrm{Aut}_{\mathbb{F}_p}(K) = \mathrm{Gal}(K/\mathbb{F}_p)$
7. Existence et unicité "du" corps fini à $q = p^n$ éléments

1. K comme ensemble des racines de $X^q - X$

Théorème

Soit K un corps fini de cardinal $card(K) = q$. Alors $(\forall x \in K) \qquad x^q = x$, *et donc :*

$$X^q - X = \prod_{a \in K} (X - a) \qquad \in K[X]$$

Démonstration :

1. $(K^*, *, e)$ est un groupe d'ordre $q - 1$, donc $(\forall x \in K^*) \qquad x^{q-1} = e$, et finalement : $(\forall x \in K) \qquad x^q = x$.
2. Le polynôme $X^q - X \in K[X]$ admet comme racines distinctes les q éléments de K. Comme K est intègre, $X^q - X$ est divisible par $\prod_{a \in K}(X - a)$. Comme ces deux polynômes ont même degré et ont même cœfficient dominant, ils sont égaux.

□

2. $(K^*, *, e)$ est un groupe cyclique

Théorème

Soit $(K, 0, +, *, e)$ un corps fini commutatif de cardinal $card(K) = q$. Alors $(K^*, *, e)$ est un groupe cyclique d'ordre $q - 1$.

Démonstration : Comme par hypothèse le groupe $(K^*, *, e)$ est commutatif, on peut utiliser le critère de cyclicité (revoir groupes cycliques ...).
Soit $d \in \mathbb{N}$ un diviseur de $q - 1$. Le polynôme $X^d - 1$ admet au plus d racines dans K (car K intègre). Par suite,

$$(\forall d | (q-1)) \qquad \text{card}\left\{x \in K^* : \quad x^d = e\right\} \leq d$$

$(K^*, *, e)$ est donc cyclique d'ordre $q - 1$. □

3. K admet un élément primitif sur $\mathbb{F}_p$

Soit K un corps de caractéristique $\mathrm{car}(K) = p$ et de cardinal $q = p^n$.
$(K^*, *, e)$, groupe cyclique d'ordre $q-1$, admet $\phi(q-1)$ générateurs.

Corollaire ($K = \mathbb{F}_p(\alpha)$)

Tout générateur $\alpha \in K$ du groupe cyclique $(K^*, *, e)$ est un élément primitif de l'extension $K/\mathbb{F}_p$:

$$K = \mathbb{F}_p(\alpha)$$

Démonstration :

1. $\mathbb{F}_p(\alpha)$ est le plus petit sous-corps de K contenant α (et bien sûr $\mathbb{F}_p$), en particulier $\mathbb{F}_p(\alpha) \subset K$.
2. $K = \{0\} \cup K^* = \{0; e; \alpha; \ldots; \alpha^{q-2}\} \subset \mathbb{F}_p(\alpha)$.

□

Attention : Les $\phi(q-1)$ générateurs de K^* sont des éléments primitifs de $K/\mathbb{F}_p$. L'inverse est FAUX : un élément primitif de $K/\mathbb{F}_p$ peut ne pas engendrer K^*.

4. $K = \mathbb{F}_p[X]/(P)$, où $P \in \mathbb{F}_p[X]$ est irréductible

Soit K un corps de caractéristique $\mathrm{car}(K) = p$ et de cardinal $q = p^n$.

Théorème ($K = \mathbb{F}_p[X]/(P)$)

Soient $\alpha \in K$ et P_α son polynôme minimal sur $\mathbb{F}_p$.

$$K = \mathbb{F}_p(\alpha) \iff K = \mathbb{F}_p[X]/(P_\alpha) \iff \deg(P_\alpha) = n$$

Démonstration : découle de $\boxed{\mathrm{card}\left(\mathbb{F}_p[X]/(P_\alpha)\right) = p^{\deg(P_\alpha)}}$ et de la factorisation :

$$\begin{array}{ccc} \mathbb{F}_p[X] & \xrightarrow{\varphi_\alpha} & K \\ \pi \downarrow & & \uparrow \\ \mathbb{F}_p[X]/(P_\alpha) & \xrightarrow{\widetilde{\varphi_\alpha}} & \mathbb{F}_p(\alpha) \end{array}$$

□

5. Les sous-corps de K

Soit K un corps de caractéristique $\mathrm{car}(K) = p$ et de cardinal $q = p^n$.

Théorème (les sous-corps de K)

1. *Tout sous-corps de K est de caractéristique p et de cardinal p^d où $d|n$.*
2. *Pour tout diviseur d de n, il existe un unique sous-corps de K de cardinal p^d, c'est :*

$$K_d \overset{déf}{=} \left\{ x \in K : \quad x^{p^d} = x \right\}$$

Démonstration :

1. Si K' est un sous-corps de K, on a $\mathbb{F}_p \hookrightarrow K' \hookrightarrow K$. D'où $\mathrm{car}(K') = p$, l'existence de $d \in \mathbb{N}$ tel que $\mathrm{card}(K') = p^d$, puis de $n' \in \mathbb{N}$ tel que $(p^d)^{n'} = p^n$.
2. Soit $d \in \mathbb{N}$. Avec $x^{p^d} = \mathrm{Frob}_K^d(x)$, $K_d \overset{\text{déf}}{=} \left\{ x \in K : \quad x^{p^d} = x \right\}$ est un sous-corps de K. Si $d|n$, il est de cardinal p^d. (unicité en exercice) □

6. Le groupe des automorphismes de K est $\mathrm{Aut}_{\mathbb{F}_p}(K) = \mathrm{Gal}(K/\mathbb{F}_p)$

Soit K un corps de caractéristique $\mathrm{car}(K) = p$ et de cardinal $q = p^n$.

Théorème (le groupe des automorphismes de K)

1. *Tout automorphisme du corps K laisse $\mathbb{F}_p$ invariant.*
2. *$Aut_{\mathbb{F}_p}(K)$, le groupe des automorphismes de K, est cyclique d'ordre n, engendré par $Frob_K : x \mapsto x^p$.*

Démonstration :

1. Si $f : K \to K$ est un morphisme, $f(0) = 0$, $f(e) = e$, $f(k \cdot e) = k \cdot e$ pour $k = 2, \ldots, p-1$.
2. Frob_K est un automorphisme de K tel que $\mathrm{Frob}_K^n = \mathrm{Id}_K$, donc l'ordre de Frob_K est n (exercice).
   Soit $\alpha \in K$ tel que $K = \mathbb{F}_p(\alpha)$. Un morphisme $f : K \to K$ est déterminé par $f(\alpha)$, qui est une racine de P_α. Donc $\mathrm{Aut}_{\mathbb{F}_p}(K)$ est d'ordre au plus n.

□

7. Existence et unicité "du" corps fini à $q = p^n$ éléments

Soient $p \in \mathbb{P}$ et $n \in \mathbb{N}$, $n \geq 1$.
2^e hypothèse provisoire : Il existe des $P \in \mathbb{F}_p[X]$ irréductibles, de degré n.

Théorème ("Le" corps fini à $q = p^n$ éléments)

1. *Il existe un corps fini K à $q = p^n$ éléments.*
2. *Deux corps finis à $q = p^n$ éléments sont isomorphes.*

"Le" corps fini à q éléments est souvent désigné par $\mathbb{F}_q$.

Démonstration :

1. On choisit $P \in \mathbb{F}_p[X]$ irréductible, de degré n. Alors $K = \mathbb{F}_p[X]/(P)$ est un corps à p^n éléments.
2. Soient K et L deux corps à $q = p^n$. Alors K et L sont deux extensions de degré n de $\mathbb{F}_p$. Soit $\alpha \in K$ un élément primitif de $K/\mathbb{F}_p$ et $P = P_\alpha \in \mathbb{F}_p[X]$ son polynôme minimal. Ainsi K est isomorphe à $\mathbb{F}_p[X]/(P)$. Mais L est aussi isomorphe à $\mathbb{F}_p[X]/(P)$ (exercice).

□

Sur la non unicité de l'isomorphisme ...

Soient $p \in \mathbb{P}$ et $n \in \mathbb{N}$, $n \geq 1$.
Soient K et L deux corps à $q = p^n$ éléments.

Théorème (les n isomorphismes entre 2 corps à $q = p^n$ éléments)

1. *Si $f : K \to L$ et $g : K \to L$ sont deux isomorphismes, alors il existe $k \in [\![0, n-1]\!]$ tel que $g = f \circ Frob_K^k$.*
2. *Soit $f_0 : K \to L$ un isomorphisme et posons $f_k = f_0 \circ Frob_K^k$. Alors les n isomorphismes $f_k : K \to L$ pour $k \in [\![0, n-1]\!]$ sont deux à deux distincts.*

Démonstration :

1. $f^{-1} \circ g \in \mathrm{Aut}(K)$ qui est engendré par Frob_K.
2. Frob_K est d'ordre n.

□